PureVPN's OpenVPN Setup Guide for pfSense (2.4.4)

pfSense is an open source firewall and router that is available completely free of cost. It offers load balancing, unified threat management, multi WAN, and other features for those particularly concerned about their online security and privacy.

Fortunately, users can further enhance its capabilities via PureVPN's OpenVPN, which can be setup on the latest pfSense (2.4.4).

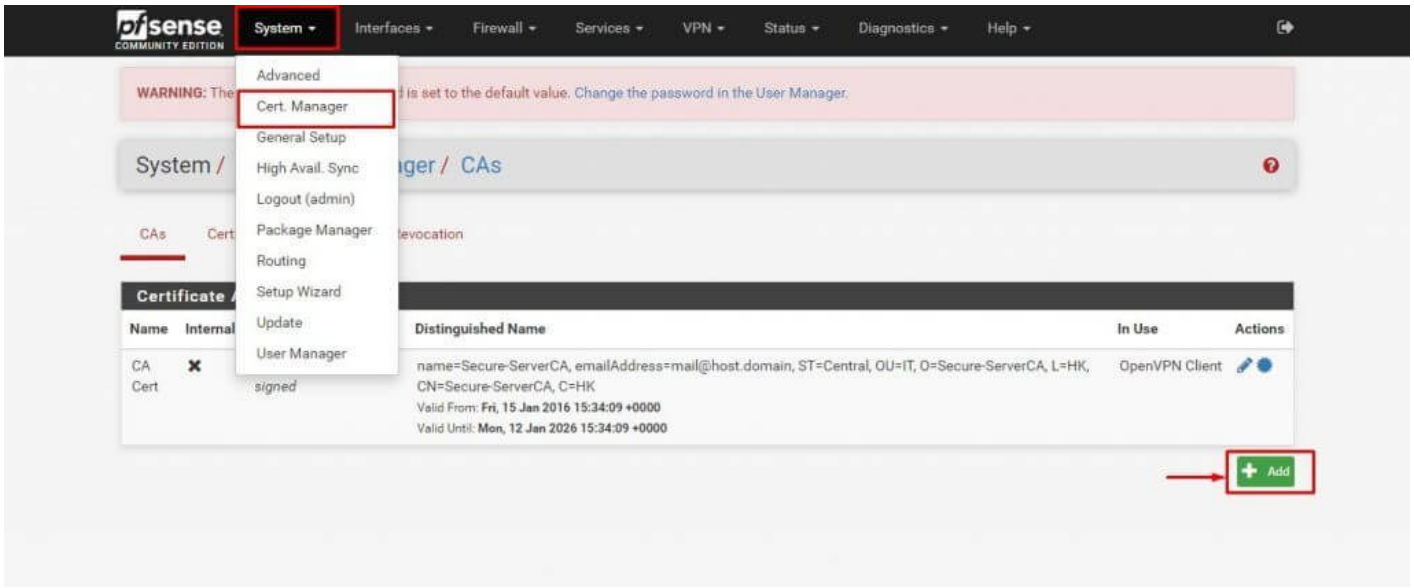
Things to Consider:

Before you begin, please make sure that you have:

- A working internet connection
- A VPN-supported router.
- A premium PureVPN account (If you do not already own one, you can buy a subscription from purevpn.com)

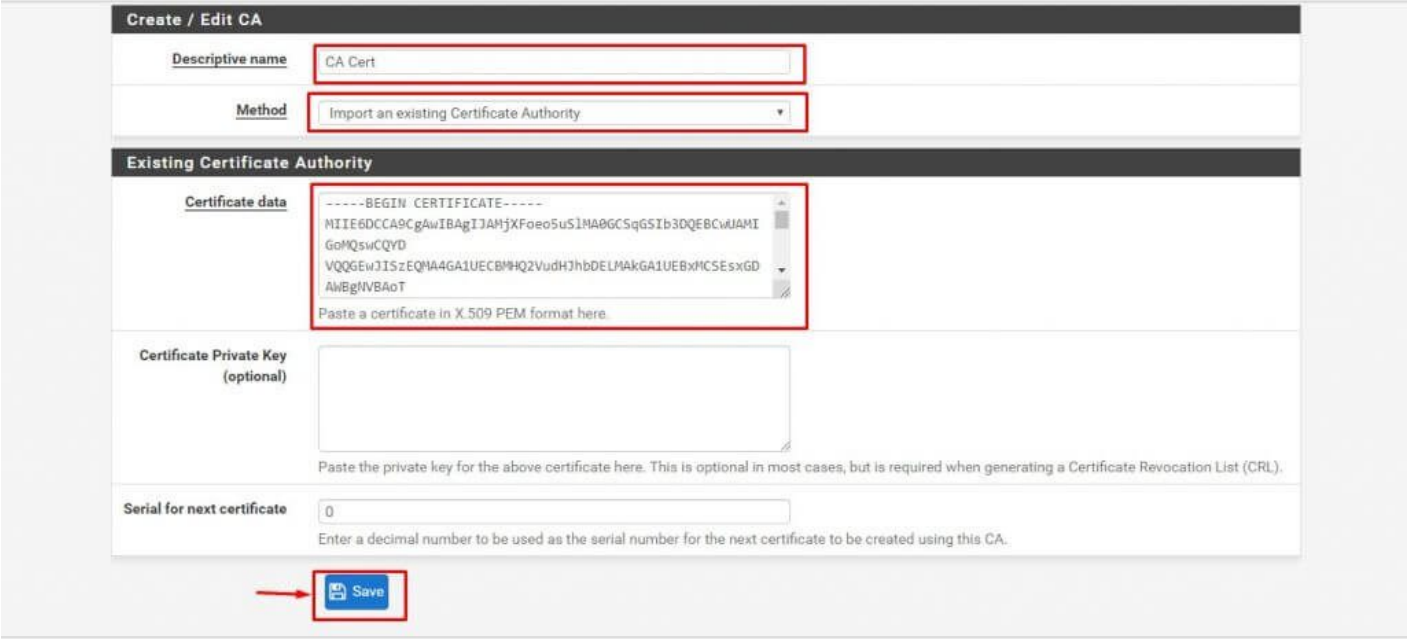
1 In order to configure OpenVPN on pfSense, first download the required OpenVPN Files from here and extract them.

2 After accessing your pfSense account, look for **Cert Manager** under **System** and click **+** to add a new certificate.



3 Now, input the following information:

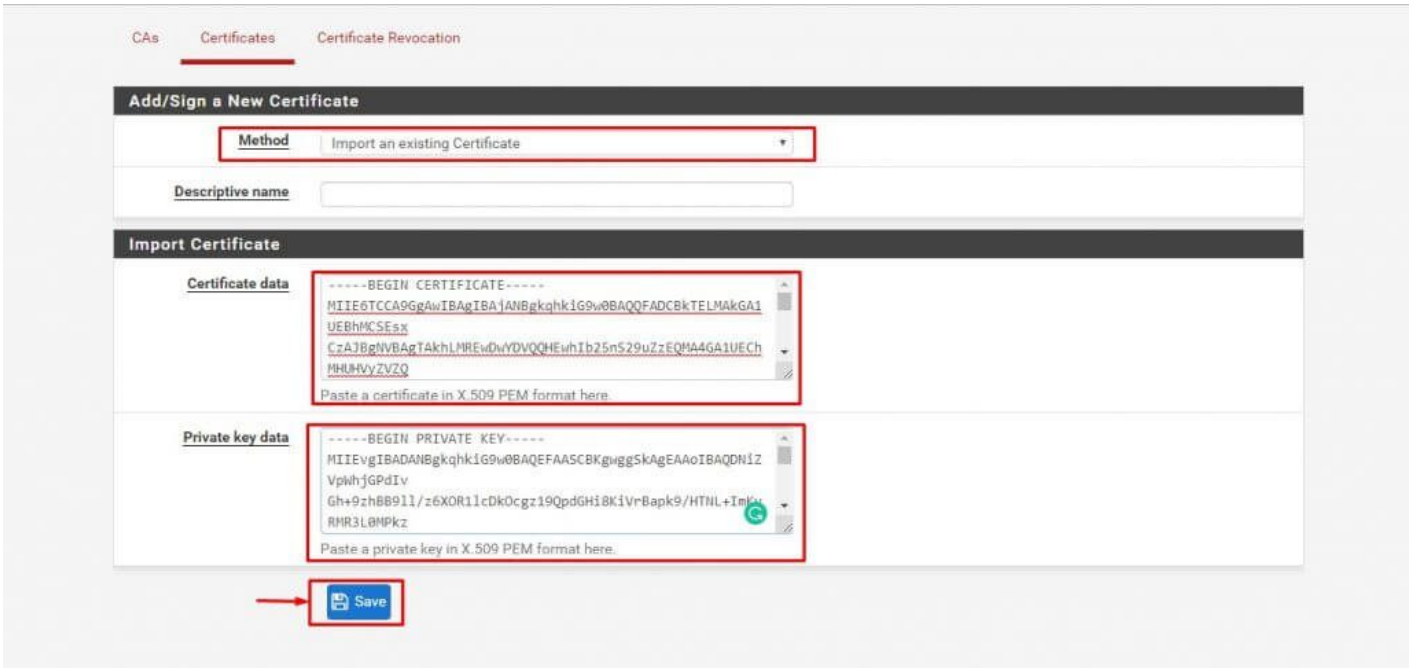
- Descriptive name: Enter **CA Cert**
- Certificate data: After downloading the necessary OpenVPN files, copy its content from **Open CA2.crt** and paste it.
- Once done, click the **Save** button.



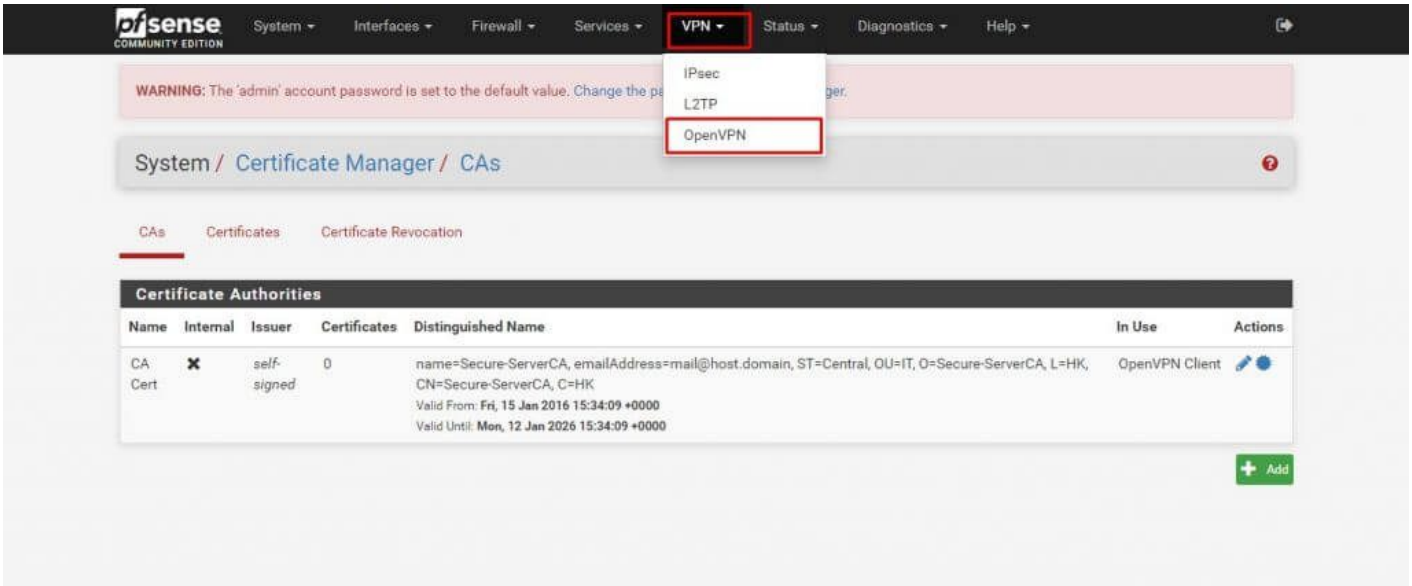
4 Select the **Certificates** tab and then click the **+** icon. Input the following information:

- Descriptive name: Enter **Client Cert**.
- Certificate data: After downloading the necessary OpenVPN files, copy its content from **Open Client.crt** and paste it.
- **Private key data:** From the downloaded OpenVPN files, access **Open Client.key**, copy its content and paste it.

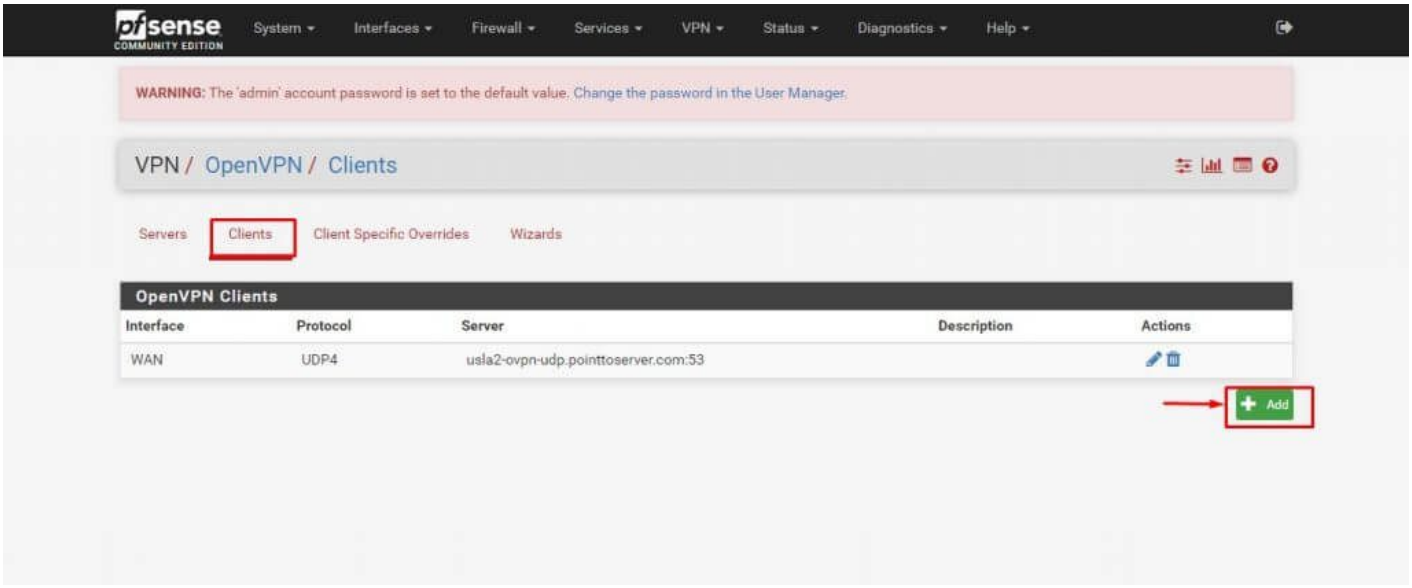
Once done, click **Save**.



5 Select **VPN** and then choose **OpenVPN** from the drop-down menu.



6 Select the **Clients** tab and click the **+** icon.

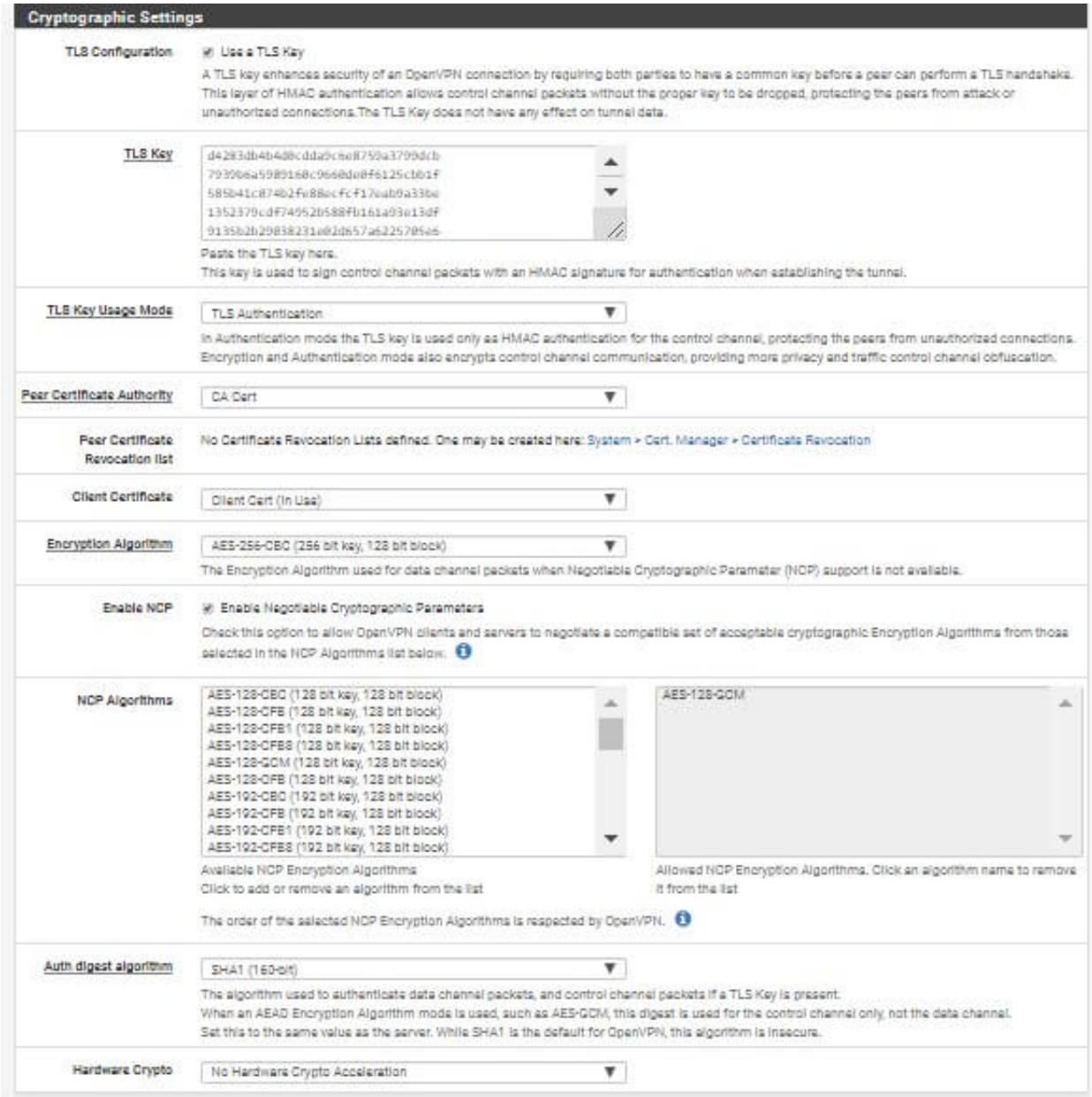


Next, input the following information:

- Server mode: **Peer-to-Peer (SSL/TLS)**
- Protocol: **UDP on IPv4 only** or **TCP on IPv4 only**
- Device mode: **Tun – Layer 3 Tunnel Mode**
- Interface: **WAN**
- Server host or address: Enter any OpenVPN server address, such as **usla2-ovpn-udp.pointtoserver.com**
- Server port: Depending on the protocol previously selected (**80** for **TCP** or **53** for **UDP**) select the appropriate port number
- User Authentication Settings: Enter your **PureVPN username and password**

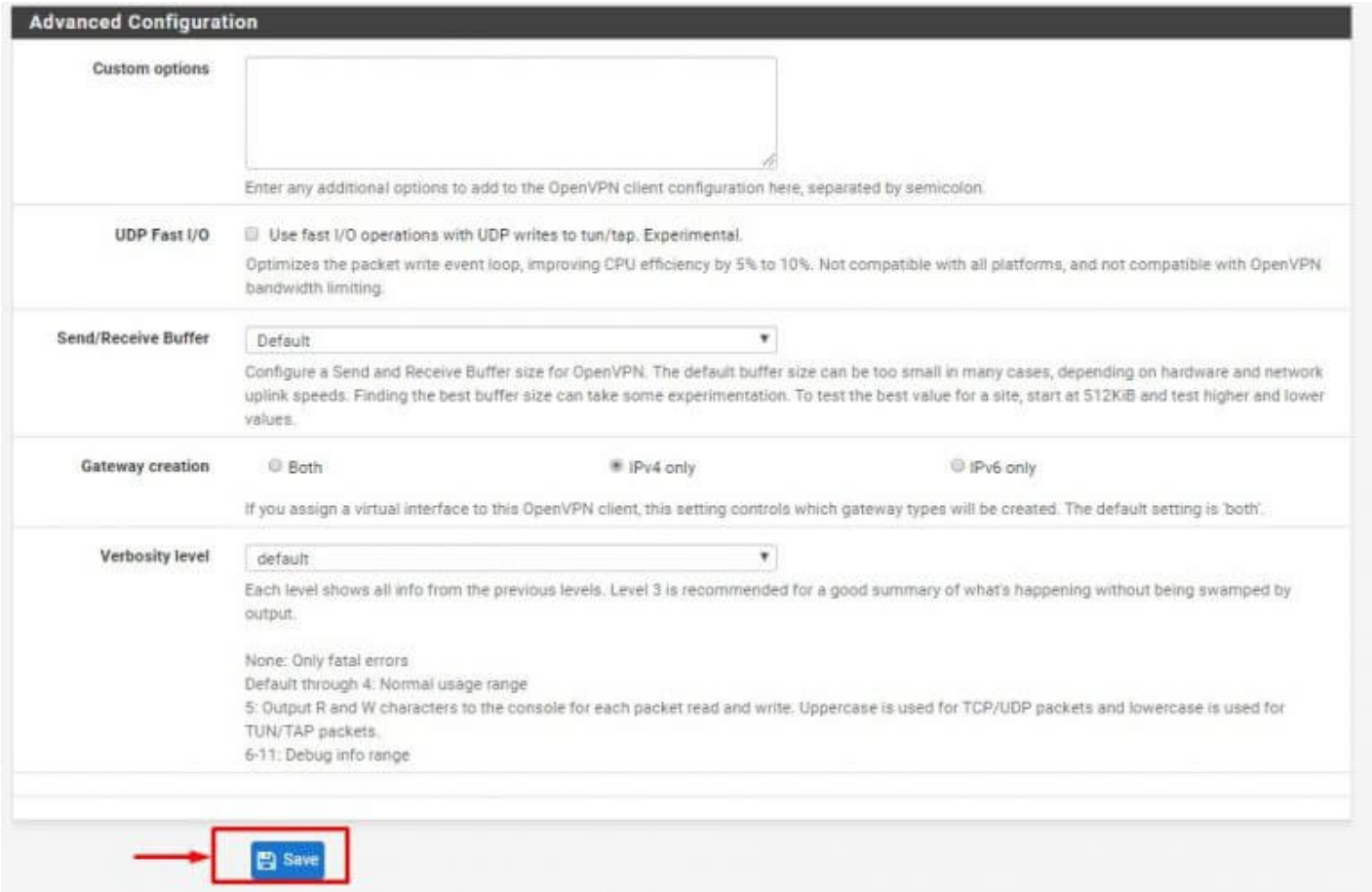
Under Cryptographic settings, do the following:

- Check the **Use a TLS Key** box next to **TLS Configuration**
- Access **Open WDC.key**. Copy and paste its content in the next box
- TLS Key Usage Mode: Choose **TLS Authentication**
- Peer Certificate Authority: **CA Cert**
- Client Certificate: **Client Cert**
- Encryption Algorithm: **AES-256-CBC**
- Enable NCP: Check the **Enable Negotiable Cryptographic Parameters** box
- Auth digest algorithm**: SHA1 (160 bit)**
- Hardware Crypto**:** Set it to **No Hardware Crypto Acceleration**

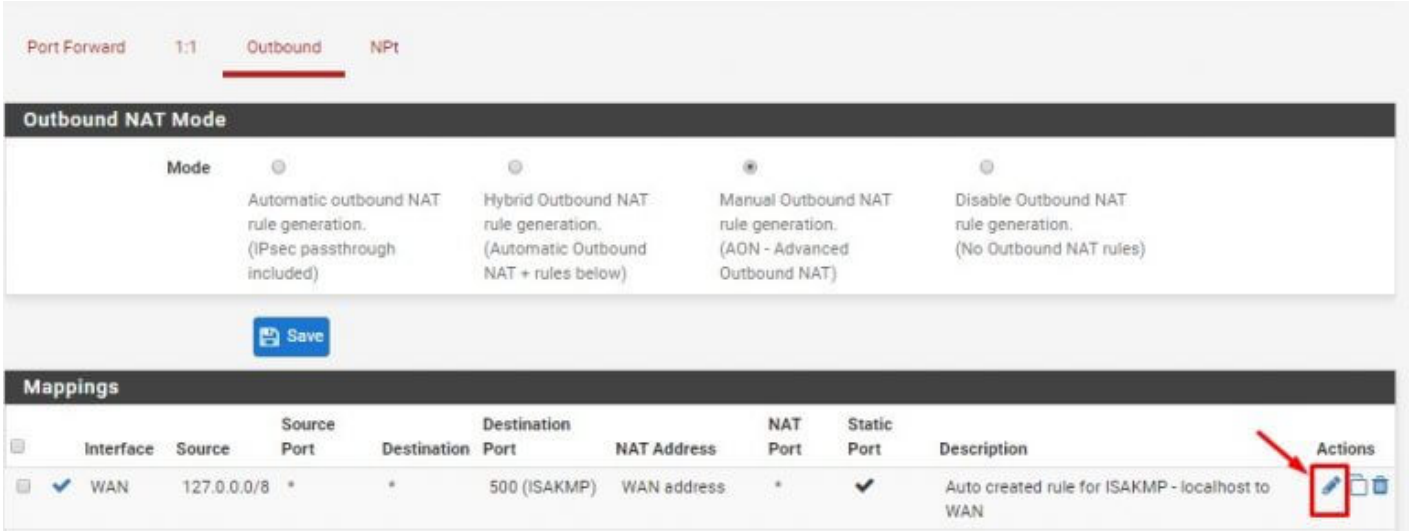


Under Advanced Settings, do the following:

- Gateway Creation: **IPv4 only**
- Click the **Save** button.

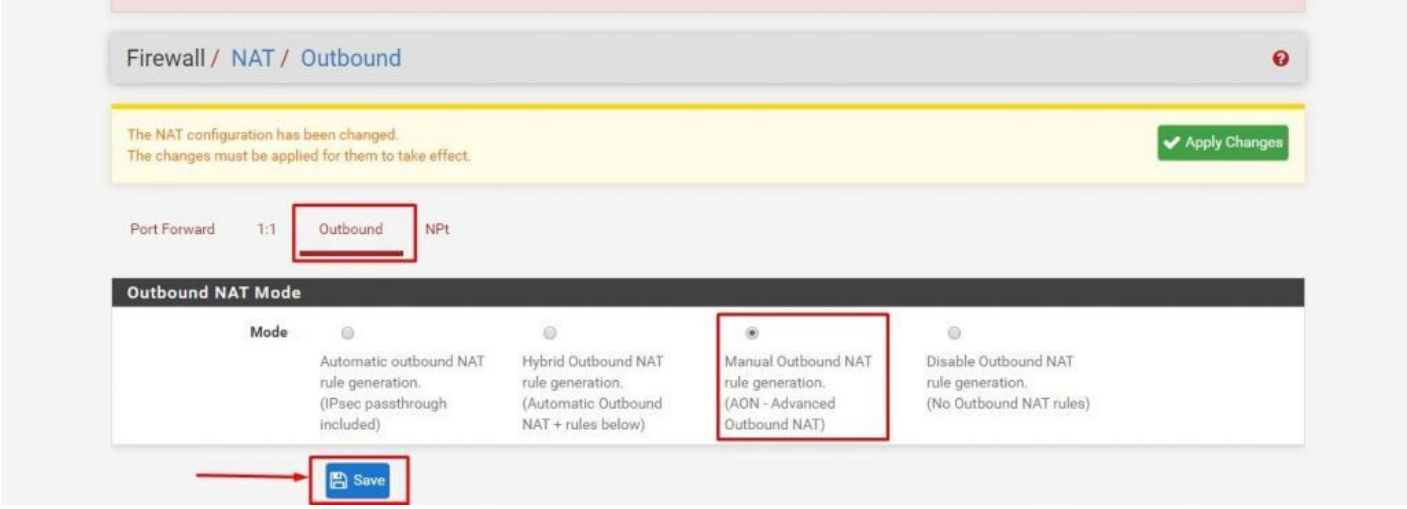


7 Under **Firewall**, click **NAT**.

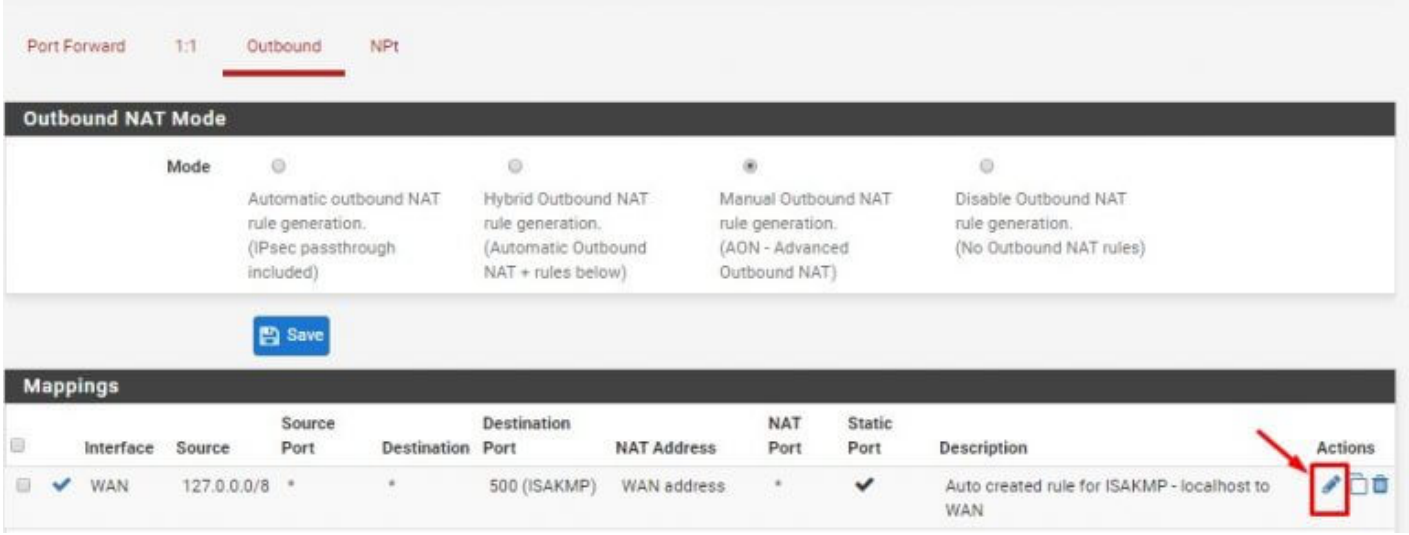


8 Select **Outbound** and then click **Manual Outbound NAT rule generation (AON Advanced**

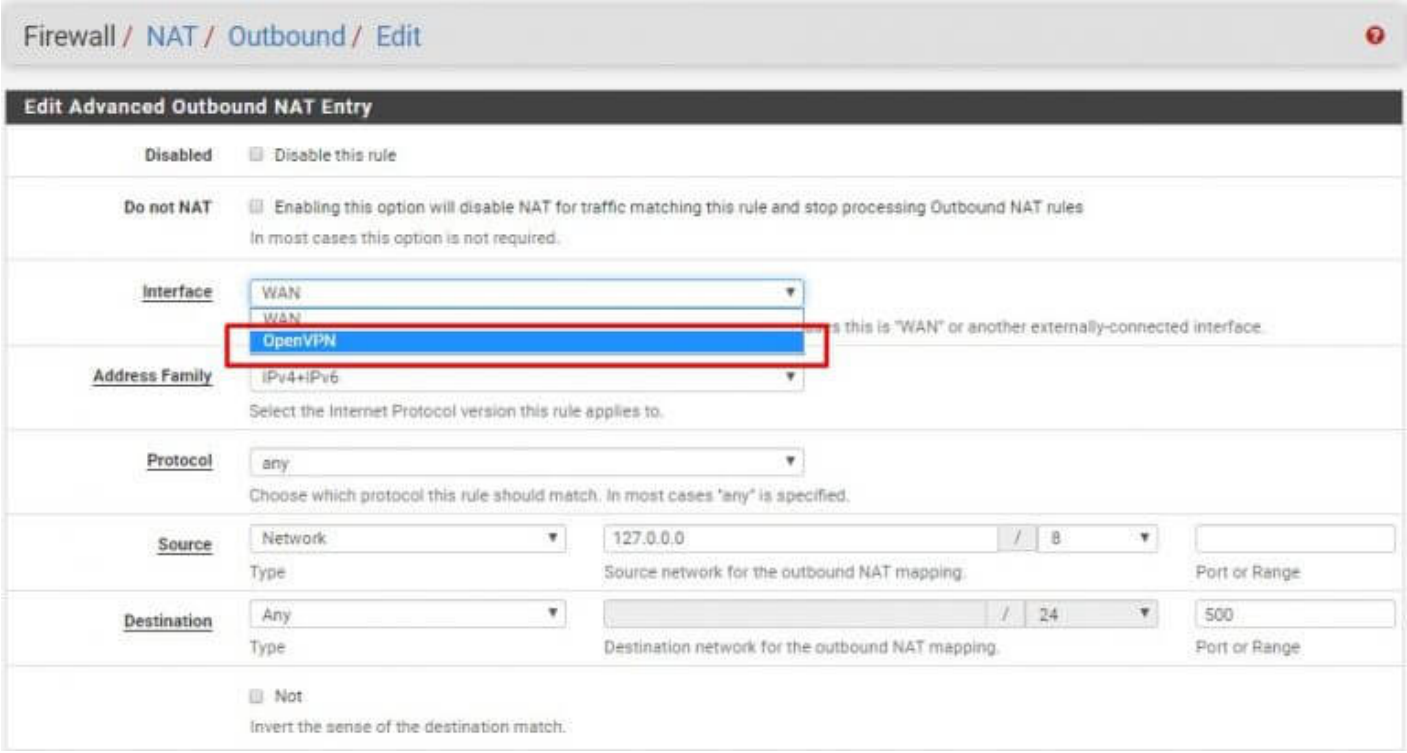
Outbound NAT) under **Outbound NAT Mode**. Click **Save** to apply changes.



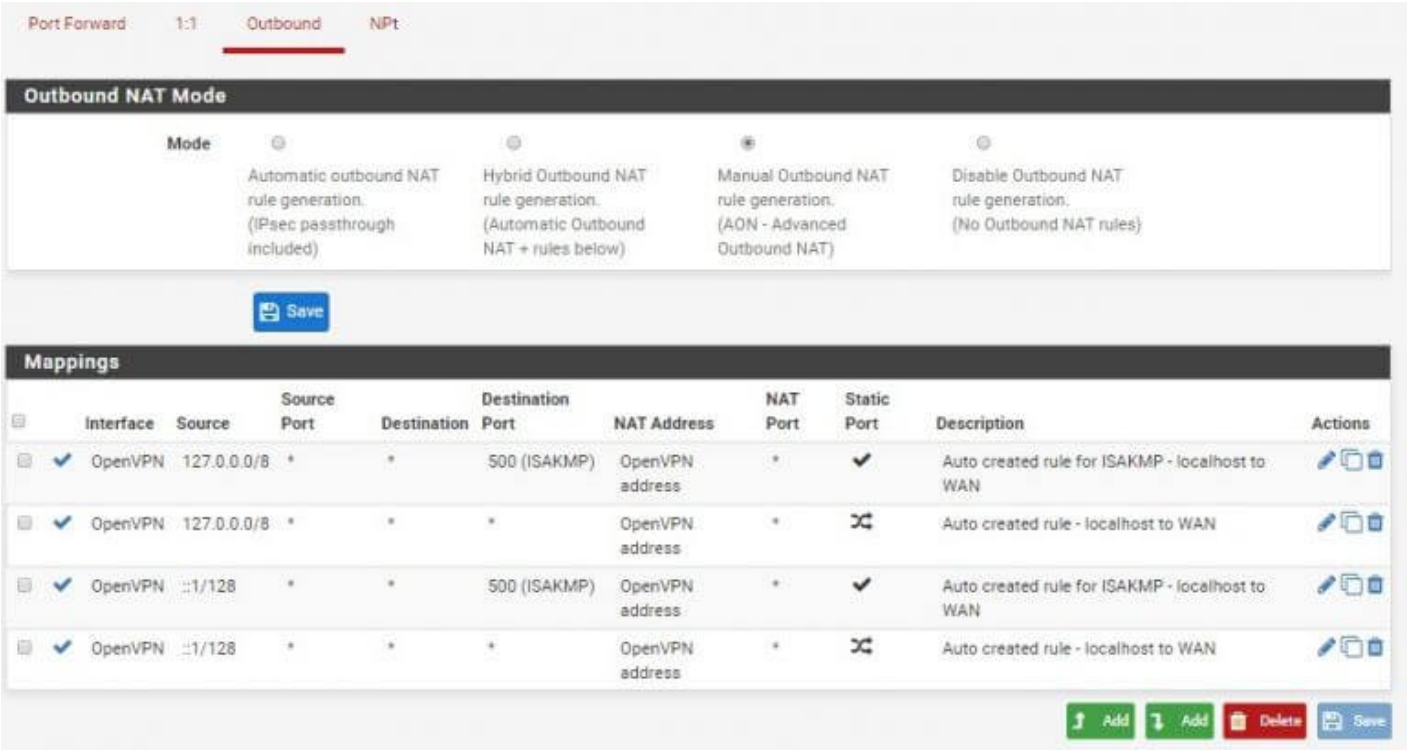
9 You will be presented with a mapping window. Each WAN perimeter within needs to be changed to OpenVPN. This can be done after clicking on the **Edit** button.



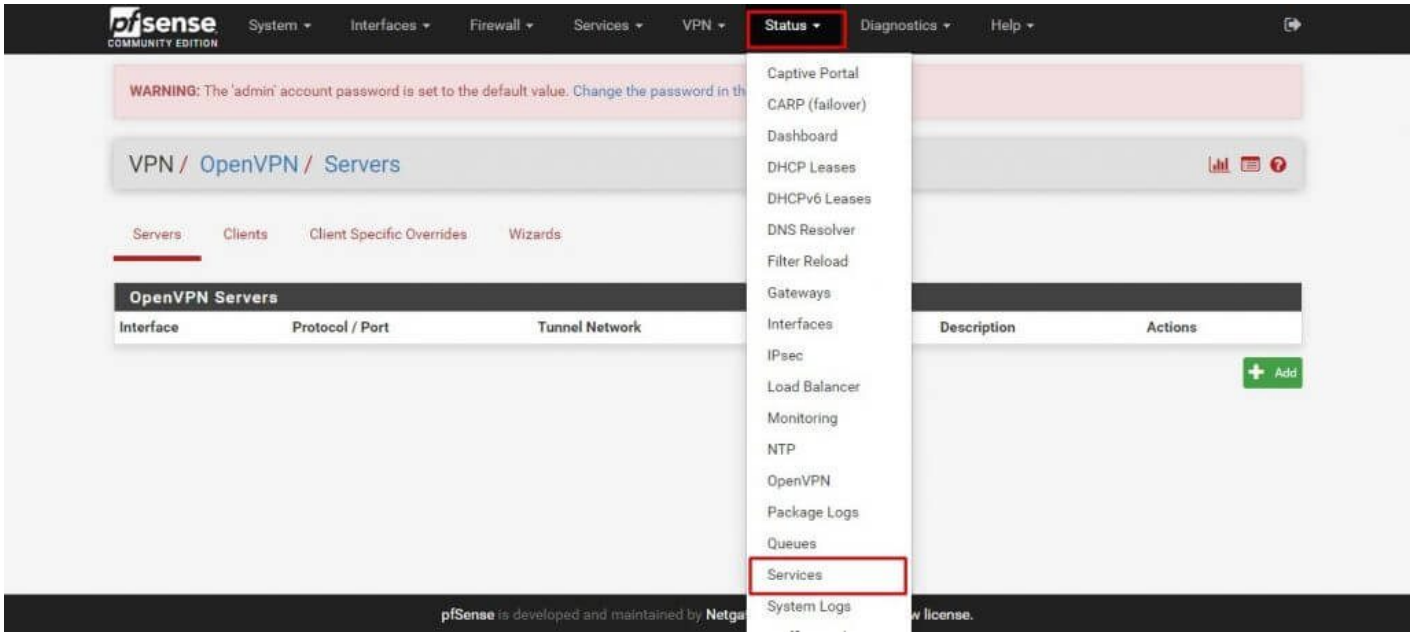
10 **Interface** needs to be changed to **OpenVPN**. Click **Save**.



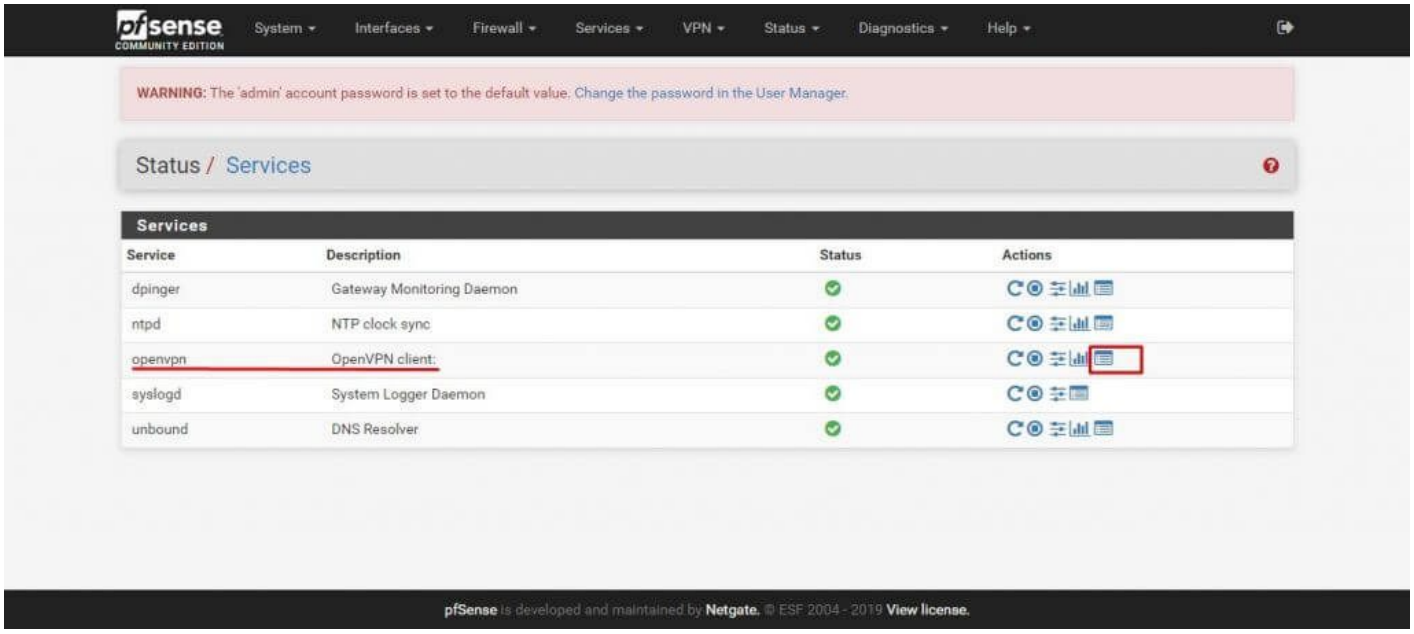
11 The above mentioned step is repeated 3 time across the board for all interfaces to OpenVPN, after which the mapping window will look something like the image below.



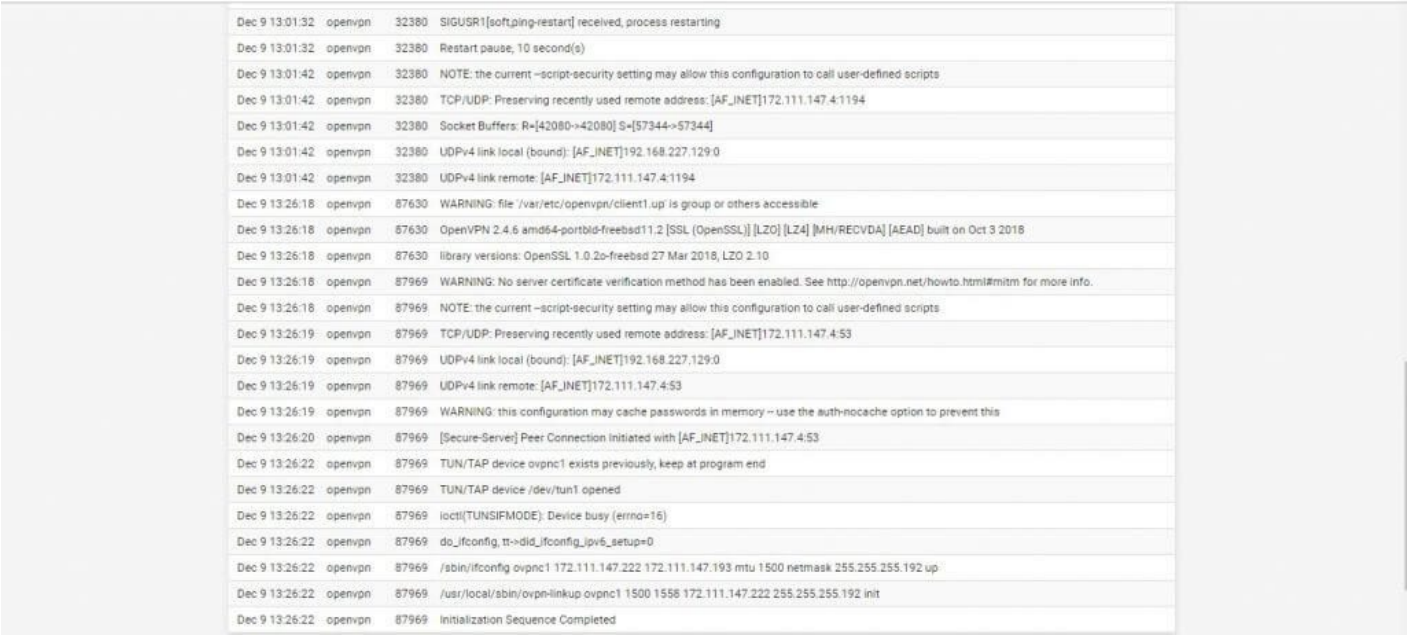
12 Click **Services** under **Status**.



13 To access OpenVPN client, click **Log Entries**.

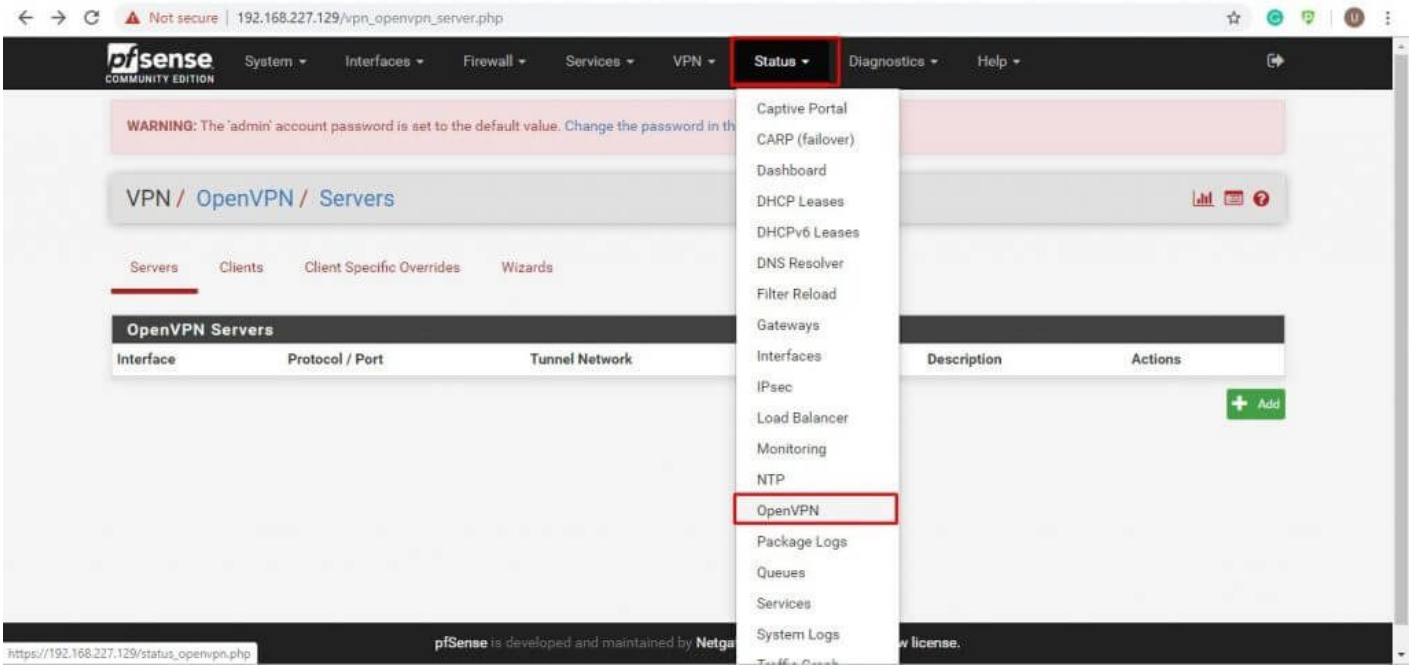


14 Once initialization is complete for the logs, it will confirm your connection.



Dec 9 13:01:32	openvpn	32380	SIGUSR1[soft,ping-restart] received, process restarting
Dec 9 13:01:32	openvpn	32380	Restart pause, 10 second(s)
Dec 9 13:01:42	openvpn	32380	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Dec 9 13:01:42	openvpn	32380	TCP/UDP: Preserving recently used remote address: [AF_INET]172.111.147.4:1194
Dec 9 13:01:42	openvpn	32380	Socket Buffers: R=[42080->42080] S=[57344->57344]
Dec 9 13:01:42	openvpn	32380	UDPv4 link local (bound): [AF_INET]192.168.227.129:0
Dec 9 13:01:42	openvpn	32380	UDPv4 link remote: [AF_INET]172.111.147.4:1194
Dec 9 13:26:18	openvpn	87630	WARNING: file '/var/etc/openvpn/client1.up' is group or others accessible
Dec 9 13:26:18	openvpn	87630	OpenVPN 2.4.6 amd64-portbld-freebsd11.2 [SSL (OpenSSL)] [LZO] [LZ4] [MH/RECVDA] [AEAD] built on Oct 3 2018
Dec 9 13:26:18	openvpn	87630	library versions: OpenSSL 1.0.2o-freebsd 27 Mar 2018, LZO 2.10
Dec 9 13:26:18	openvpn	87969	WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
Dec 9 13:26:18	openvpn	87969	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Dec 9 13:26:19	openvpn	87969	TCP/UDP: Preserving recently used remote address: [AF_INET]172.111.147.4:53
Dec 9 13:26:19	openvpn	87969	UDPv4 link local (bound): [AF_INET]192.168.227.129:0
Dec 9 13:26:19	openvpn	87969	UDPv4 link remote: [AF_INET]172.111.147.4:53
Dec 9 13:26:19	openvpn	87969	WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Dec 9 13:26:20	openvpn	87969	[Secure-Server] Peer Connection Initiated with [AF_INET]172.111.147.4:53
Dec 9 13:26:22	openvpn	87969	TUN/TAP device ovpnc1 exists previously, keep at program end
Dec 9 13:26:22	openvpn	87969	TUN/TAP device /dev/tun1 opened
Dec 9 13:26:22	openvpn	87969	ioctl(TUNSIFMODE): Device busy (errno=16)
Dec 9 13:26:22	openvpn	87969	do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Dec 9 13:26:22	openvpn	87969	/sbin/ifconfig ovpnc1 172.111.147.222 172.111.147.193 mtu 1500 netmask 255.255.255.192 up
Dec 9 13:26:22	openvpn	87969	/usr/local/sbin/ovpn-linkup ovpnc1 1500 1558 172.111.147.222 255.255.255.192 init
Dec 9 13:26:22	openvpn	87969	Initialization Sequence Completed

15 You can check status of the VPN connection from **Status** under the **OpenVPN** tab.




Status / OpenVPN
Client Instance Statistics
Name
Status
Connected Since
Local Address
Virtual Address
Remote Host
Bytes Sent/Received
Service
Client UDP4
up
Mon Dec 9 13:26:22 2019
192.168.227.129:21151
172.111.147.222
172.111.147.4:53
79 KiB / 113 KiB